IN THE CLAIMS:

Please write the claims to read as follows:

1. (Original): A policer based on Random Early Detection (RED), comprising:

a filter that determines a filtered virtual time debt; and

a control law circuit that receives the filtered virtual time debt from the filter and determines whether a packet should be dropped.

2. (Original): The RED policer of claim 1, wherein a virtual time debt uses a time T in which a packet is expected to arrive and is computed using a predetermined output transmission rate.

3. (Original): The RED policer of claim 2, wherein predetermined output transmission rate is given by a traffic contract.

4. (Currently Amended): The RED policer of claim 1, wherein the filter is based on an exponential weighted moving average (EWMA) virtual time delay using the expression,

$$EWMA_k = (1-g)EWMA_{k-1} + g(VTD)_k,$$

where k indicates the presently received packet, and k-1 indicates ~~the EWMA computed when~~ the last packet ~~was~~ received, the virtual time debt (VTD) is computed by the expression: VTD = T(packet expected to arrive) – T(packet actually arrives), and g is the gain of the filter.

5. (Original): The RED policer of claim 1, further comprises a sampler that samples a virtual time debt at a sampling interval, and transmits the sampled virtual time debt to the filter.

6. (Original): The RED policer of claim 1, further comprises:

a random generator that generates a number based on the control law circuit's determination as to whether a packet should be dropped; and

a counter that is set with the number generated by the random generator, wherein the counter counts packets passing through the RED policer up to the set number, and wherein the RED policer drops a packet when the counter has counted out the set number.

7. (Original): The RED policer of claim 6, further comprises:

the control law circuit that determines a probability of a packet being dropped based on the filtered time debt exceeding a predetermined minimum threshold, and specifies a range of numbers based on the probability; and

the random generator that randomly generates a number in the range specified by the control law circuit.

8. (Original): A policer based on Random Early Detection (RED), comprising:

means for determining a moving average of a virtual time debt; and

means for determining whether a packet should be dropped based on a value of the moving average of the virtual time debt.

9. (Original): The RED policer of claim 8, further comprises means for sampling a virtual time debt at a sampling interval, and transmitting the result to the moving average determining means.

10. (Original): The RED policer of claim 8, further comprises:

means for generating a random number based on the result of the packet dropping means; and

means for counting a number of packets passing through the RED policer up to the random number generated by the random number generating means, wherein the RED policer drops a packet when the counting means has counted out the generated random number.

11. (Original): A network device comprising:

a plurality of Random Early Detection (RED) policers, wherein each RED policer includes,

a filter that determines a filtered virtual time debt; and

a control law circuit that receives the filtered virtual time debt from the filter and determines whether a packet should be dropped; and

a packet classifier that determines which packet should go to which RED policer.

12. (Previously Presented): A method of policing packets in a network device, the method comprising the steps of:

determining a filtered virtual time debt of a traffic;

comparing the filtered virtual time debt with a predetermined minimum threshold; and if the filtered virtual time debt exceeds the minimum threshold, then

generating a random number that is used to determine which packet should be dropped.

13. (Original): The method of claim 12, wherein generating a random number further comprises the steps of:

generating the random number in a range based on a level by which the filtered virtual time debt exceeds the minimum threshold;

setting a counter with the random number; and

dropping a packet when the counter has counted out the random number.

14. (Previously Presented): A computer readable medium having instructions contained therein, which when executed by a computer performs a method comprising the steps of:

determining a filtered virtual time debt of a traffic;

comparing the filtered virtual time debt with a predetermined minimum threshold; and if the filtered virtual time debt exceeds the minimum threshold, then

generating a random number that is used to determine which packet should be dropped.

15. (Original): The medium of claim 14, wherein generating a random number further comprises the steps of:

generating the random number in a range based on a level the filtered virtual time debt exceeds the minimum threshold;

setting a counter with the random number; and

dropping a packet when the counter has counted out the random number.

16. (Previously Presented): Electromagnetic signals propagating over a computer network, said electromagnetic signals carrying instructions for execution on a processor for the practice of the method comprising the steps of:

determining a filtered virtual time debt of a traffic;

comparing the filtered virtual time debt with a predetermined minimum threshold; and if the filtered virtual time debt exceeds the minimum threshold, then

generating a random number that is used to determine which packet should be dropped.

17. (Previously Presented): A method of policing packets in a network device, the method comprising the steps of:

determining a virtual time debt of packets flowing through the network device; and

determining whether a packet should be dropped based on the virtual time debt of the packets.

18. (Previously Presented): The method as in claim 17, further comprising: determining that a packet should be dropped when a virtual time debt threshold has been reached.

19. (Previously Presented): The method as in claim 17, further comprising: determining a moving average of the virtual time debt.

20. (Previously Presented): The method as in claim 17, further comprising: calculating the virtual time debt as the difference between a time a packet is expected to arrive and a time the packet actually arrives.

21. (Previously Presented): The method as in claim 20, further comprising: calculating the time a packet is expected to arrive according to a traffic contract.

22. (Previously Presented): The method as in claim 17, further comprising: sampling the virtual time debt at a sampling interval.

23. (Previously Presented): The method as in claim 17, further comprising:

generating a random number;

counting a number of packets passing through the network device up to the random number; and

dropping a packet when the counted number reaches the random number.

24. (Currently Amended): A method of policing packets in a network device, the method comprising the steps of:

determining a virtual time debt of packets flowing through the network device, the virtual time debt computed as a ~~difference between~~delay from an expected packet arrival time established by a traffic contract ~~and~~ to an actual packet arrival time;

determining that packets should be dropped when the virtual time debt of the packets exceeds a predetermined value; and if so

choosing a packet to be dropped, the chosen packet~~[,]~~ in response to a random number; and

dropping the chosen packet.

25. (Previously Presented): The method as in claim 24, further comprising:

generating the random number

counting a number of packets passing through the network device up to the random number; and

dropping a packet when the counted number reaches the random number.

26. (Currently Amended): A policer, comprising:

means for determining a virtual time debt of packets flowing through the network device, the virtual time debt computed as a ~~difference between~~delay from an expected packet arrival time established by a traffic contract ~~and~~ to an actual packet arrival time;

means for determining that packets should be dropped when the virtual time debt of the packets exceeds a predetermined value; and if so

means for choosing a packet to be dropped, the chosen packet~~[,]~~ in response to a random number; and

means for dropping the chosen packet.

27. (Previously Presented): A computer readable media, the computer readable media containing instructions for execution in a processor for the practice of the method comprising the steps of:

determining a virtual time debt of packets flowing through the network device; and

determining whether a packet should be dropped based on the virtual time debt of the packets.

28. (Previously Presented): Electromagnetic signals propagating on a computer network, the electromagnetic signals carrying instructions for execution in a processor for the practice of the method comprising the steps of:

determining a virtual time debt of packets flowing through the network device; and

determining whether a packet should be dropped based on the virtual time debt of the packets.

Please insert the following new claims, 29 *et seq.*:

29. (New): A method of policing packets in a network device, the method comprising the steps of:

determining a virtual time debt of packets flowing through the network device, the virtual time debt computed as a delay from an expected packet arrival time to an actual packet arrival time; and

determining whether a packet should be dropped based on the virtual time debt of the packets.

30. (New): The method as in claim 29, in the event a packet should be dropped, further comprising:

generating a random number;

counting a number of packets passing through the network device up to the random number; and

dropping a packet when the counted number reaches the random number.